

FIG.1
PRIOR ART

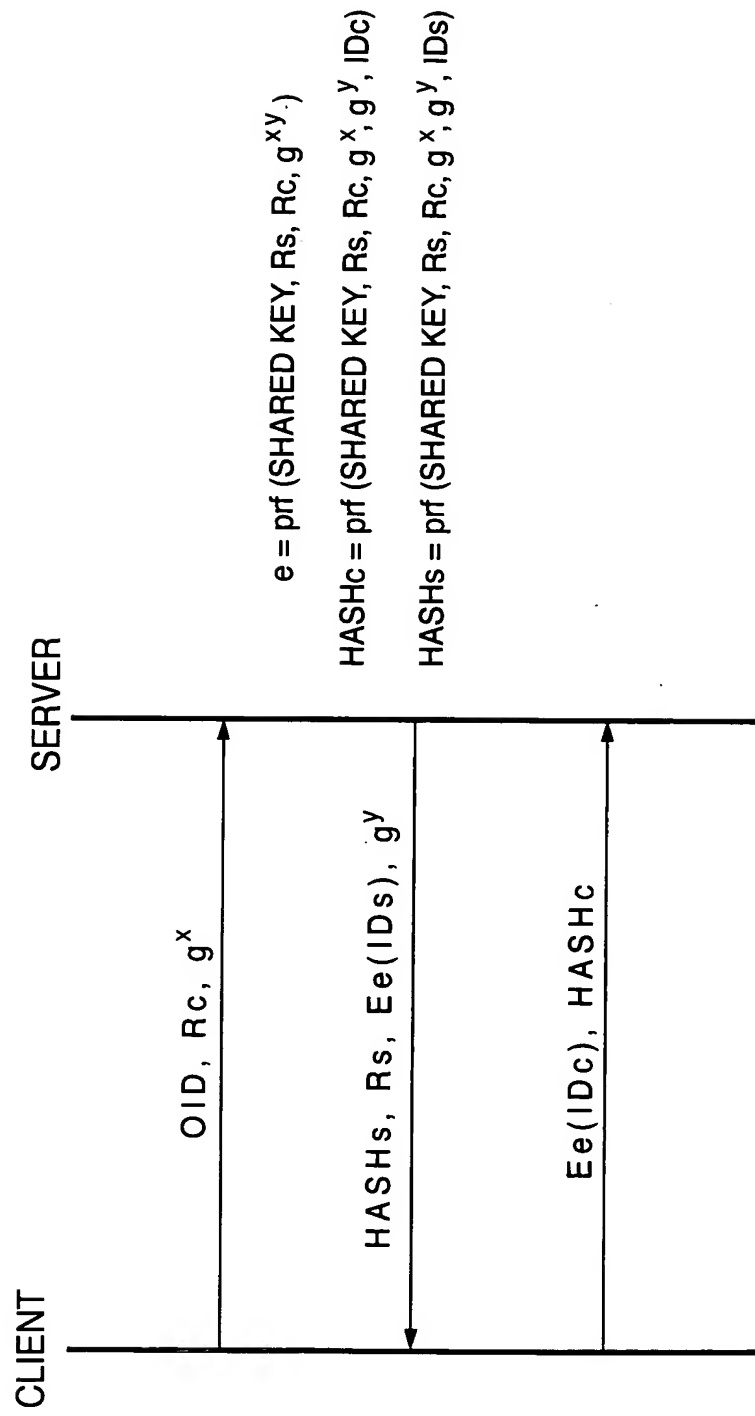


FIG.2

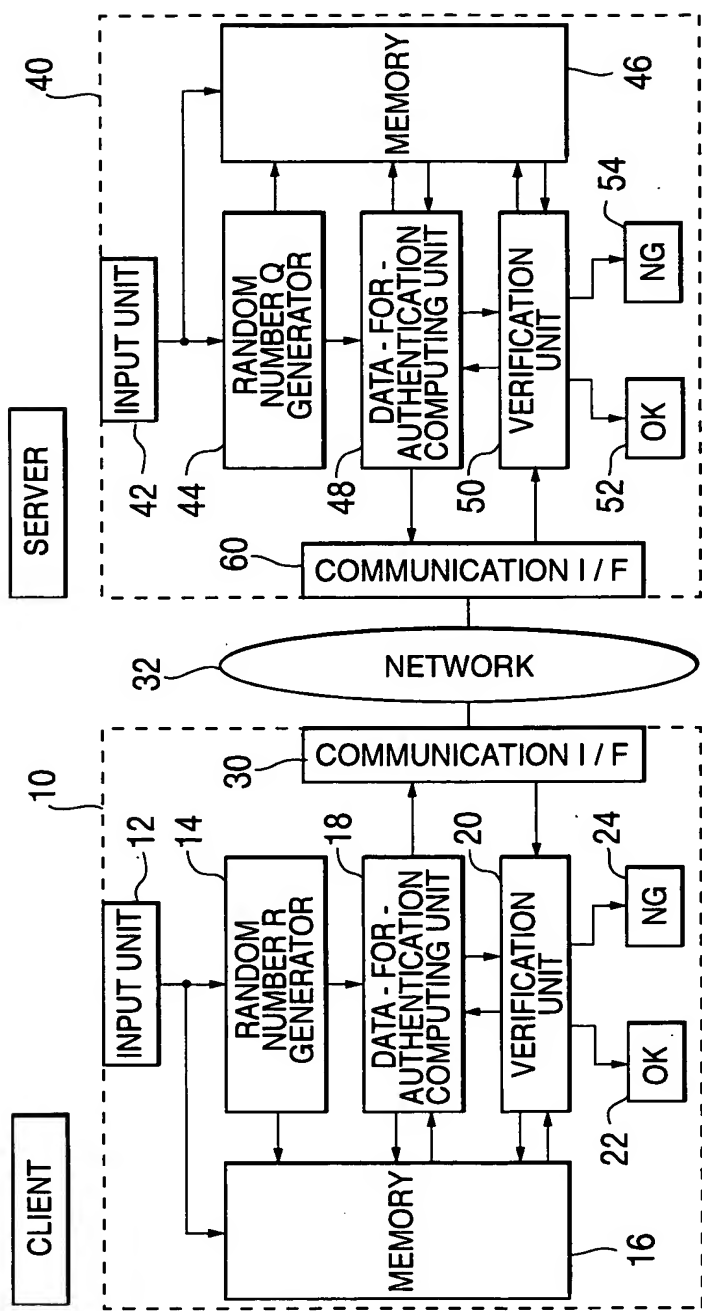


FIG.3

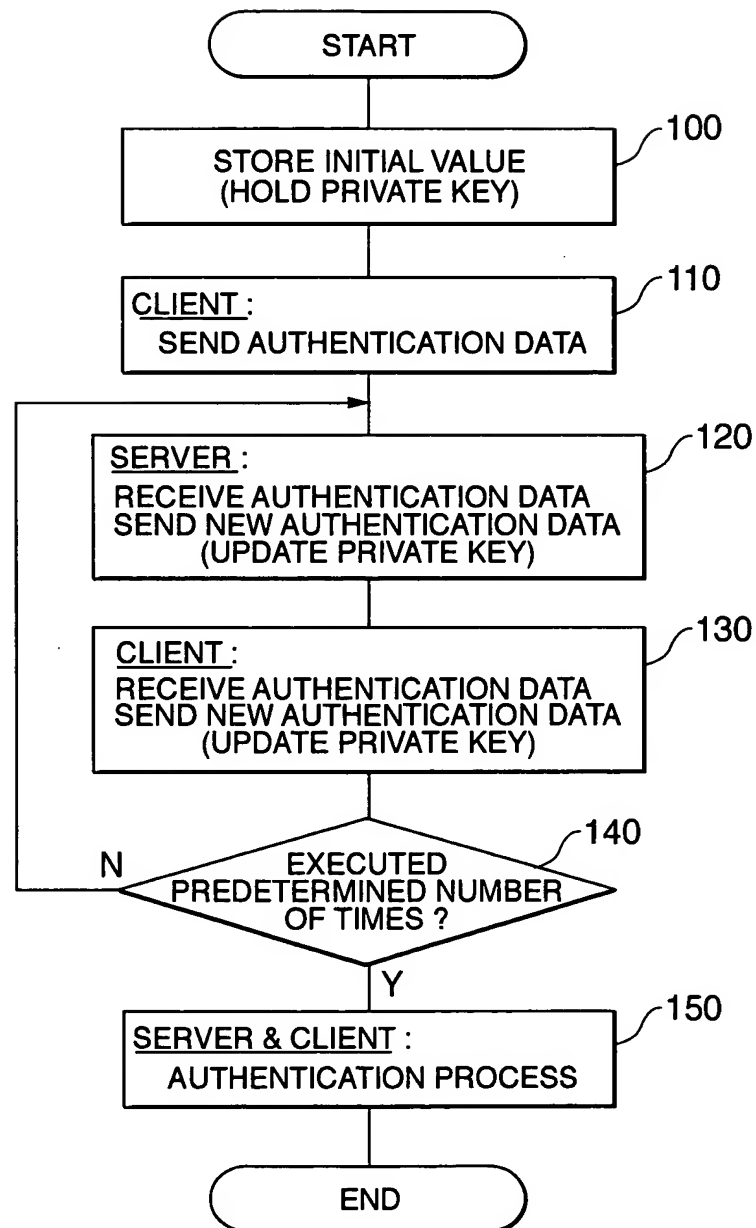


FIG. 4

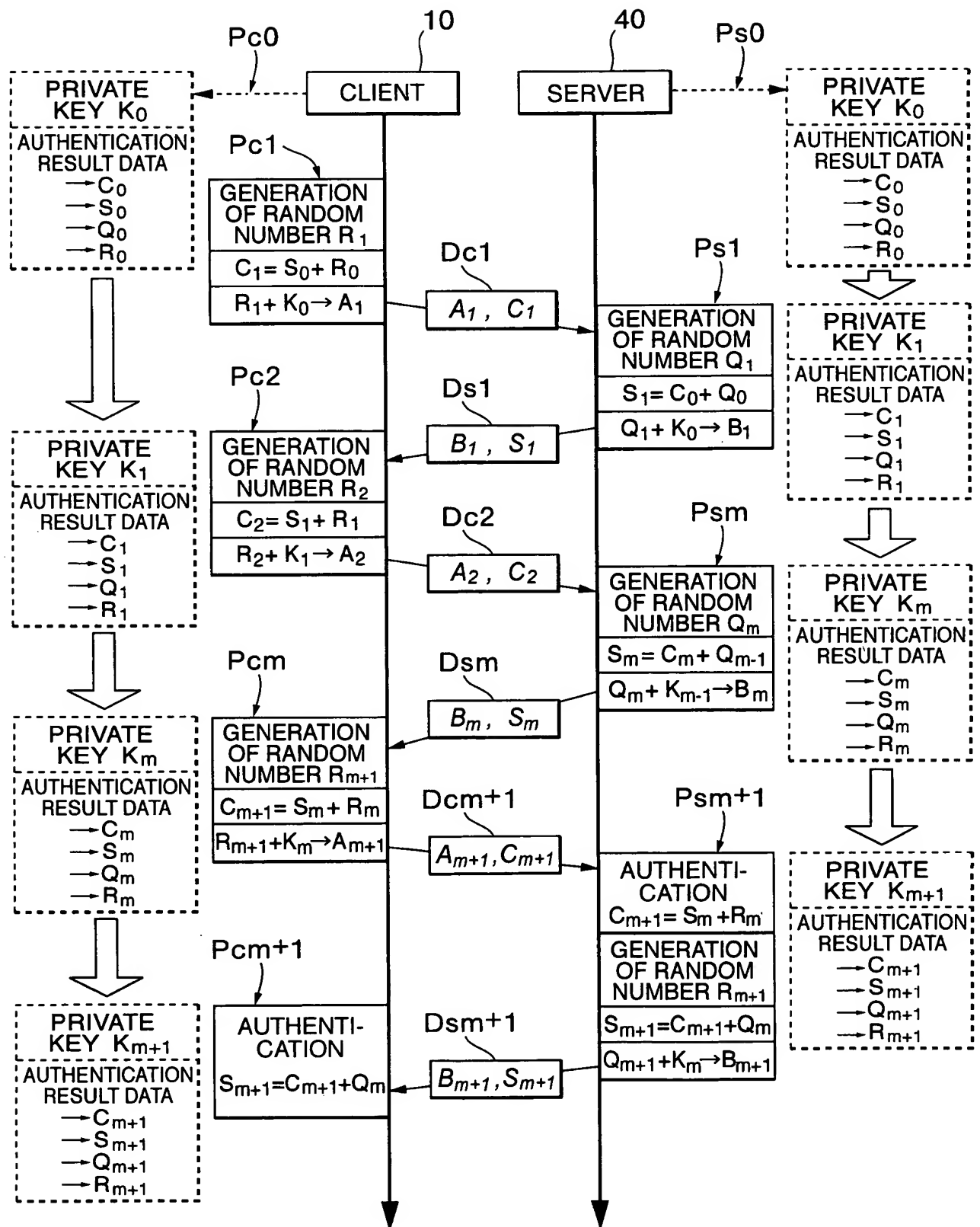


FIG. 5

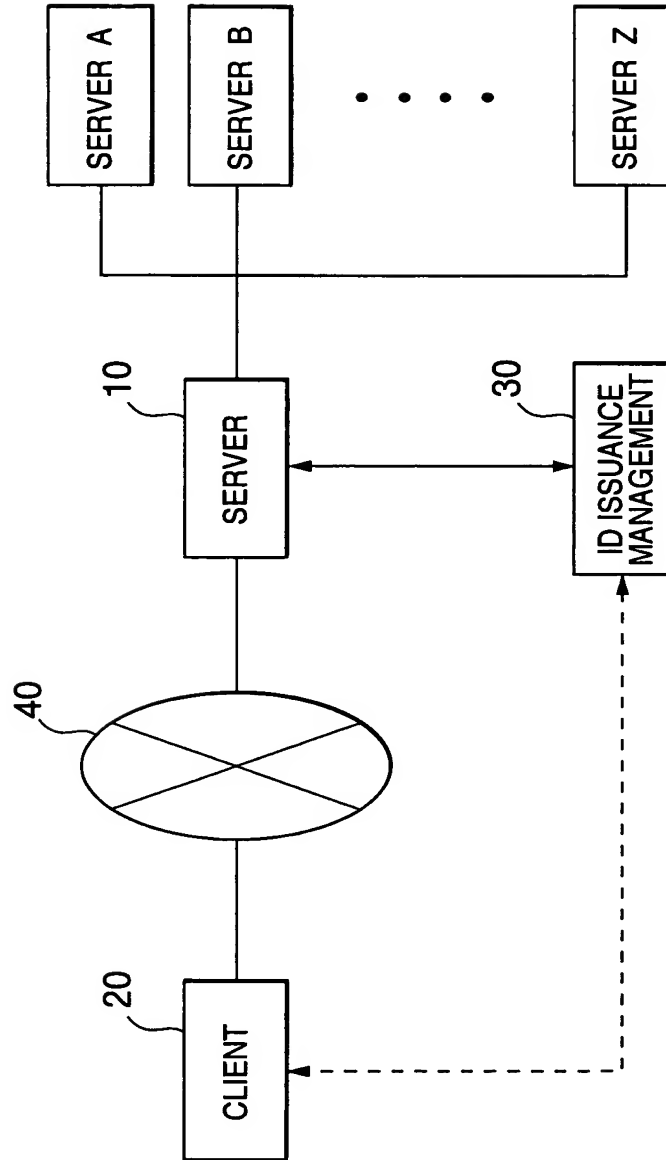


FIG.6

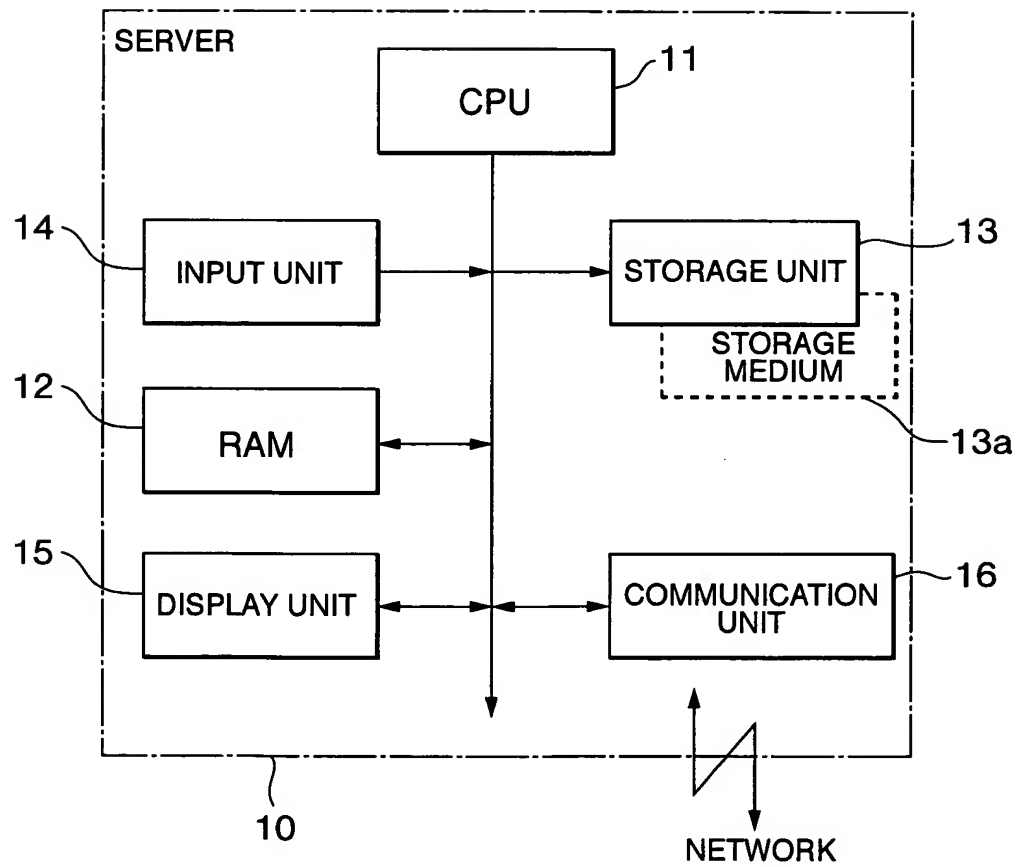


FIG.7

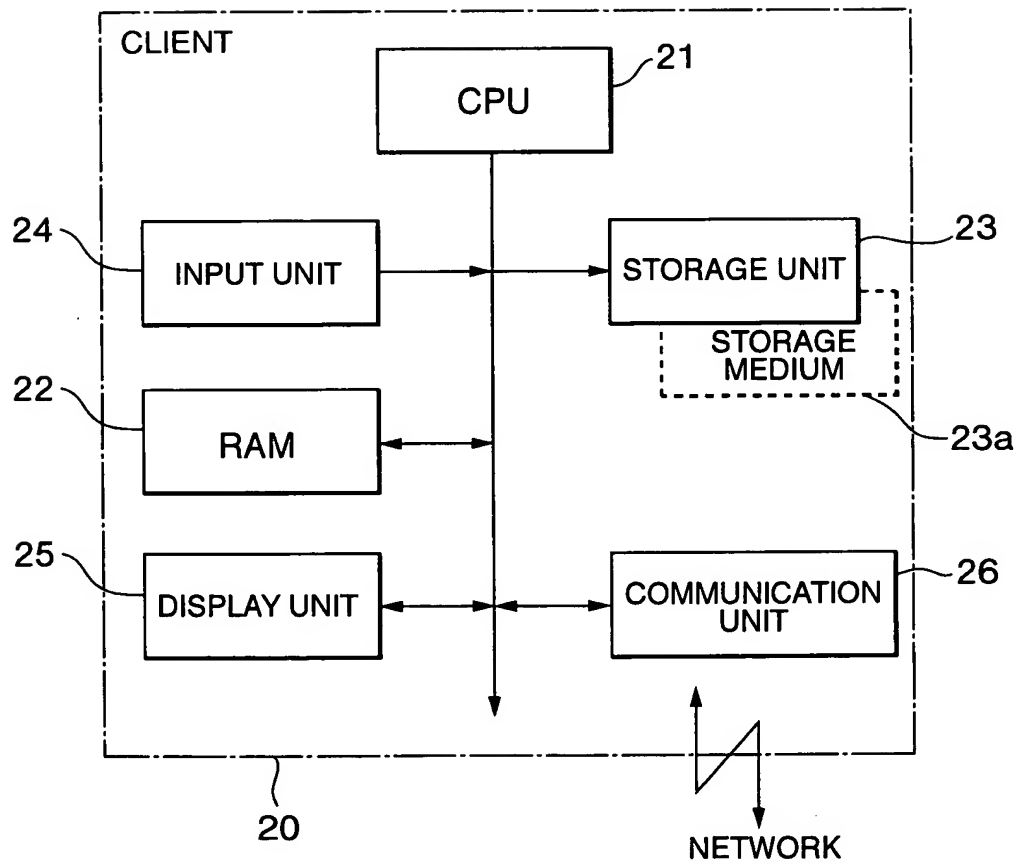


FIG.8

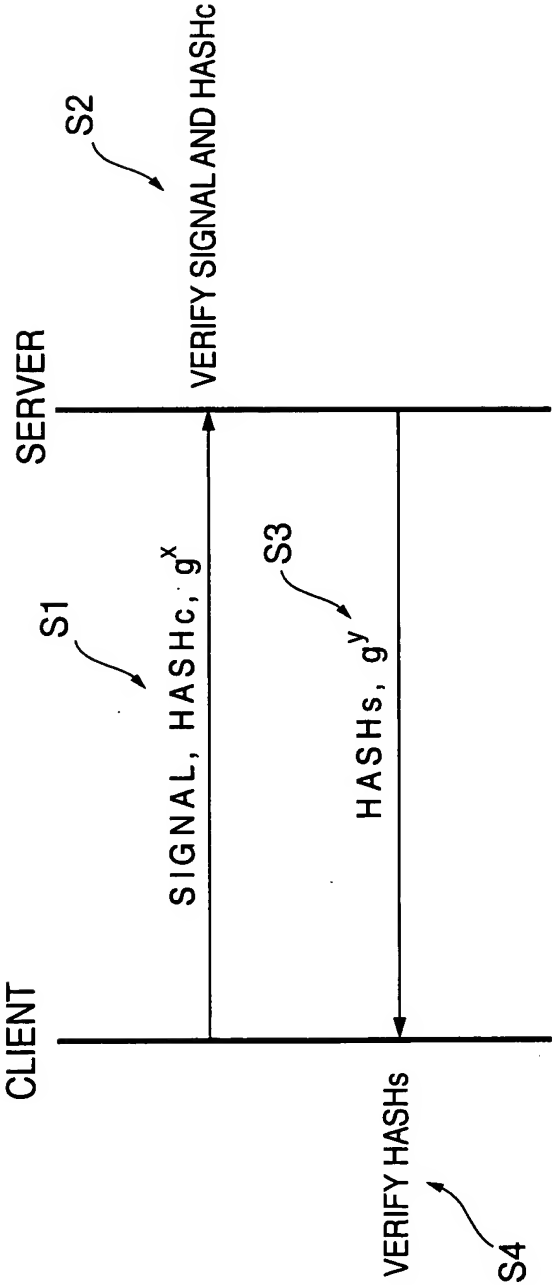


FIG.9

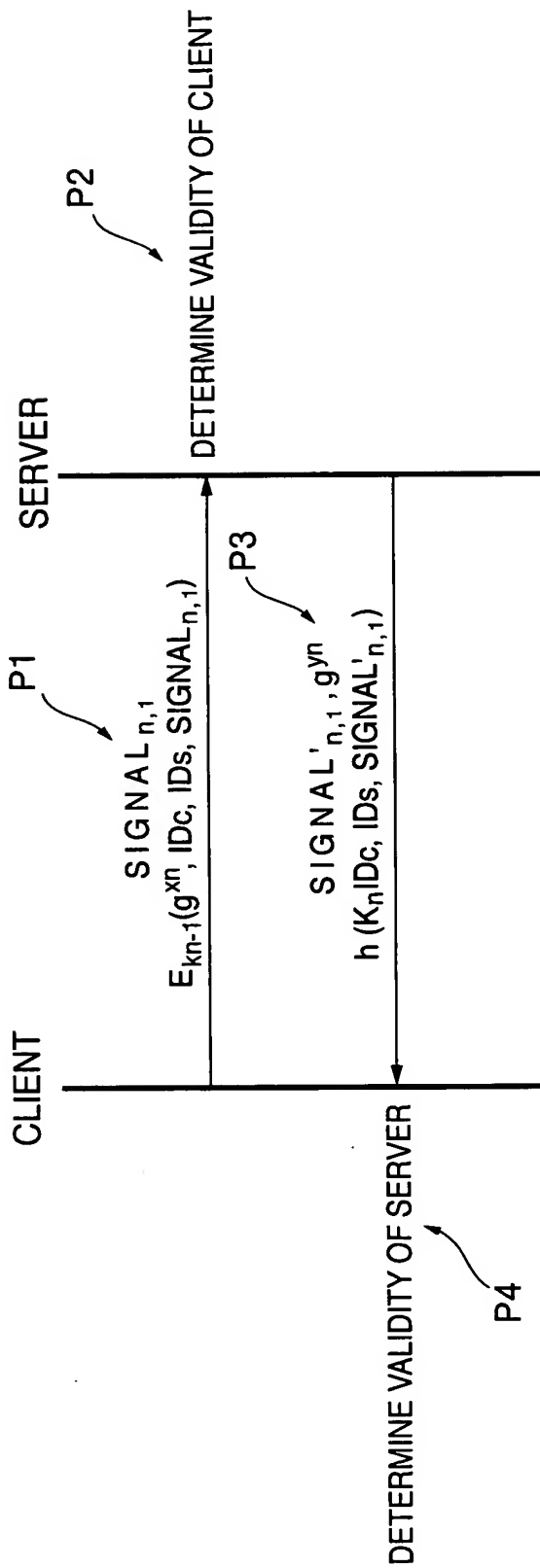


FIG.10

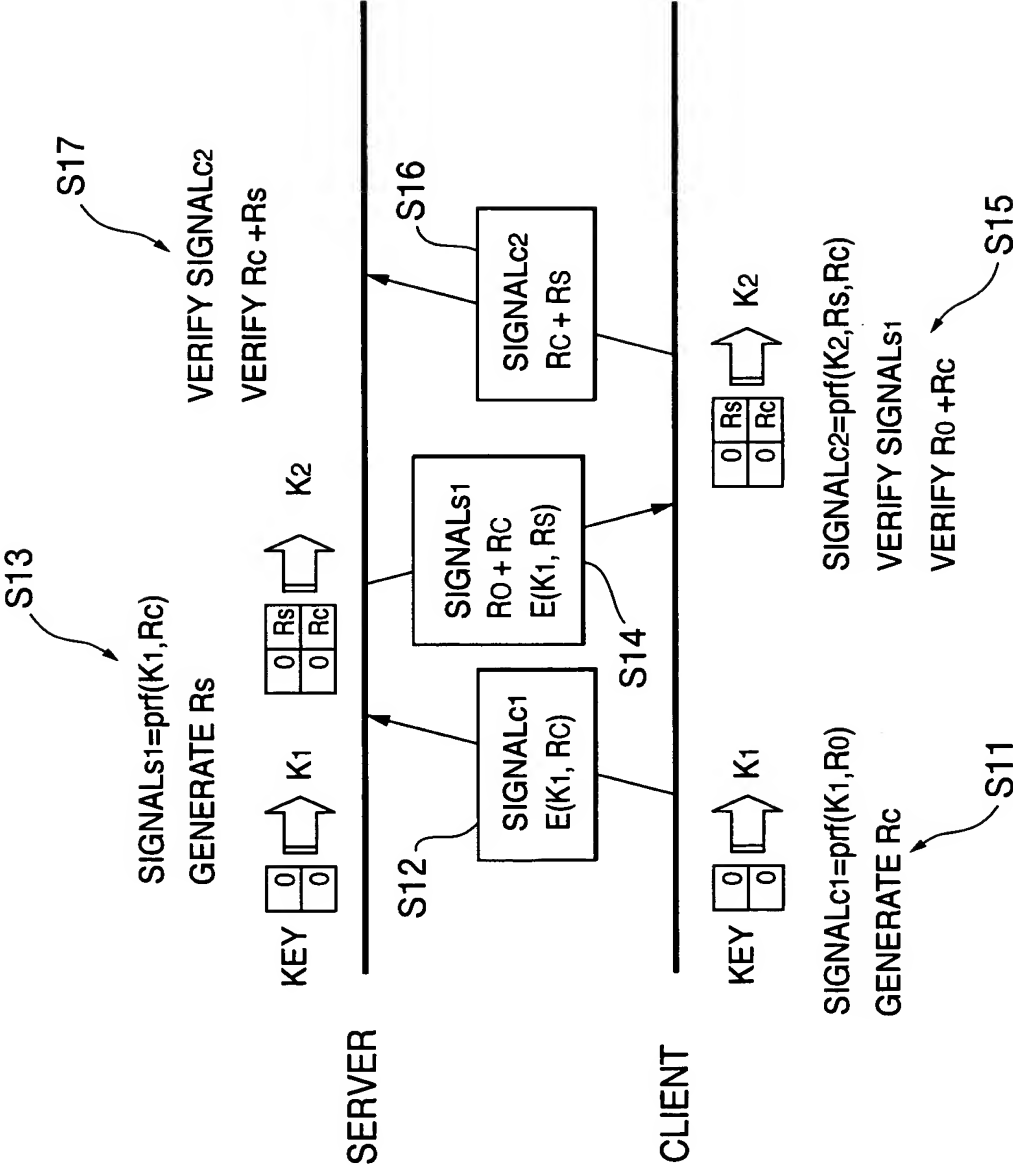


FIG.11

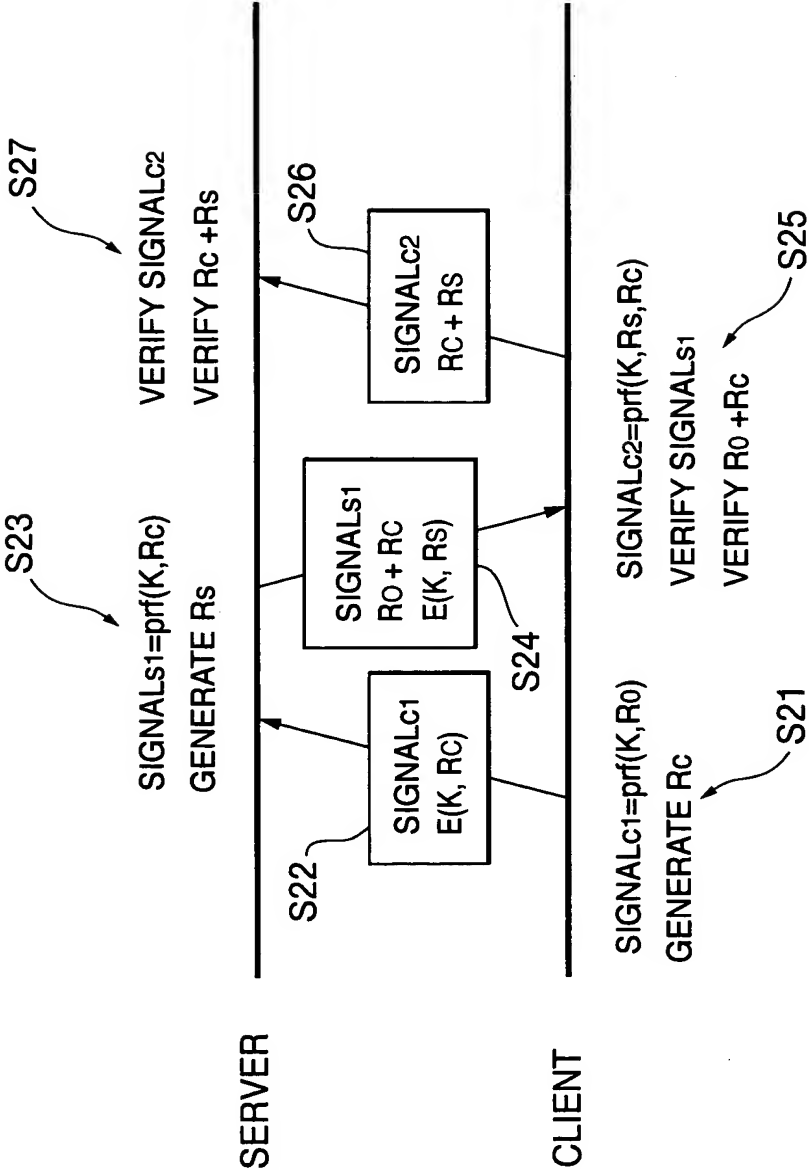


FIG.12

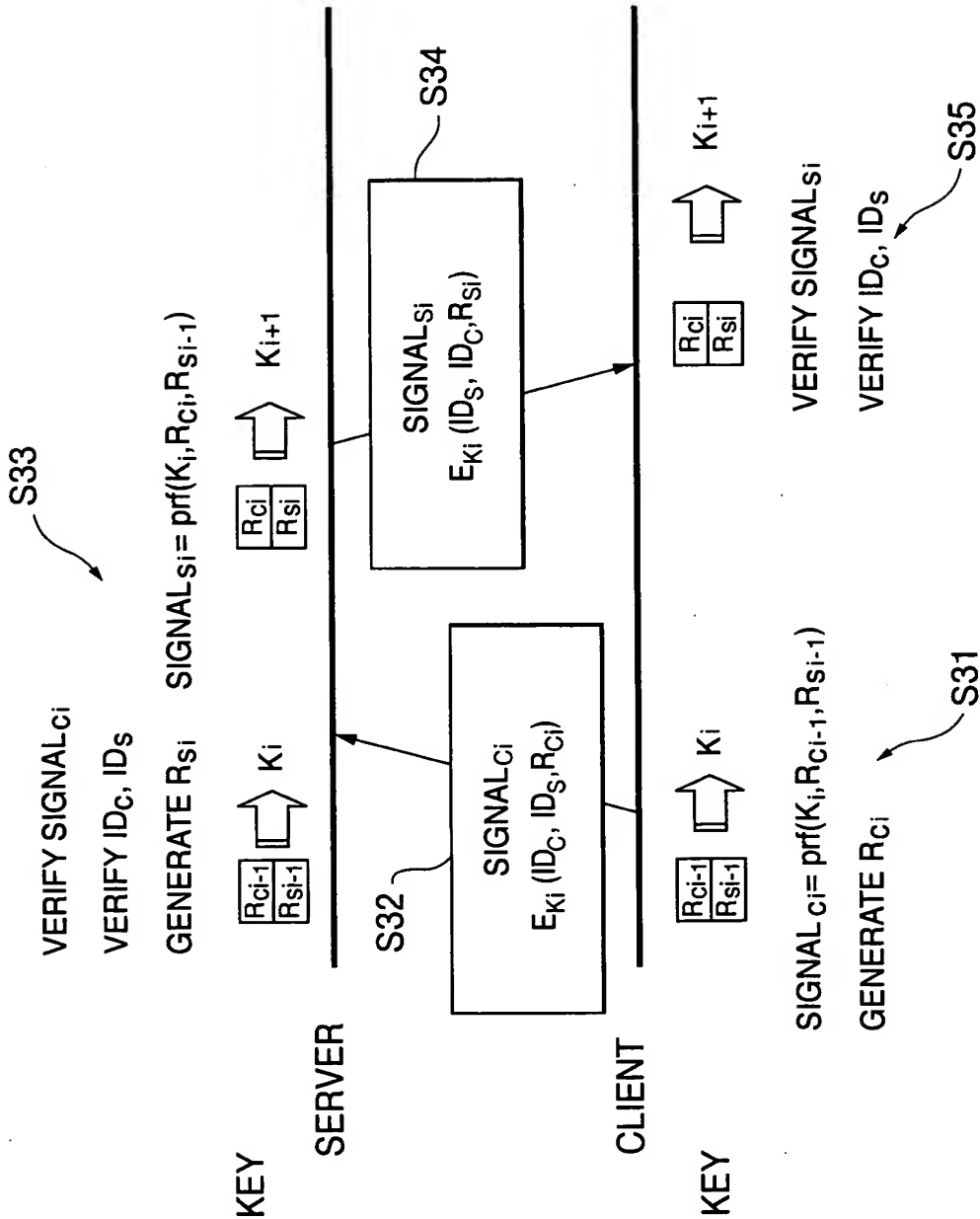


FIG.13

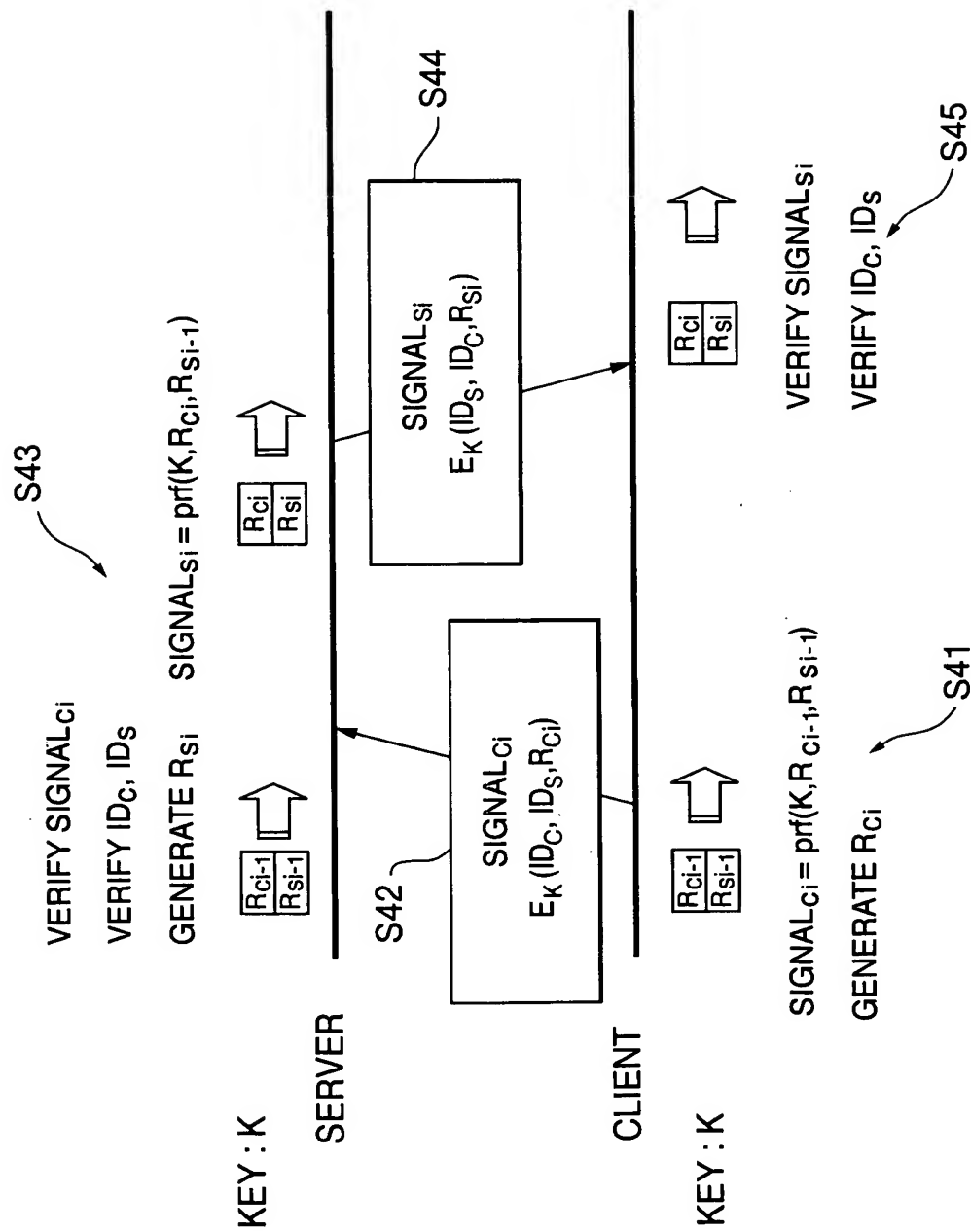


FIG.14

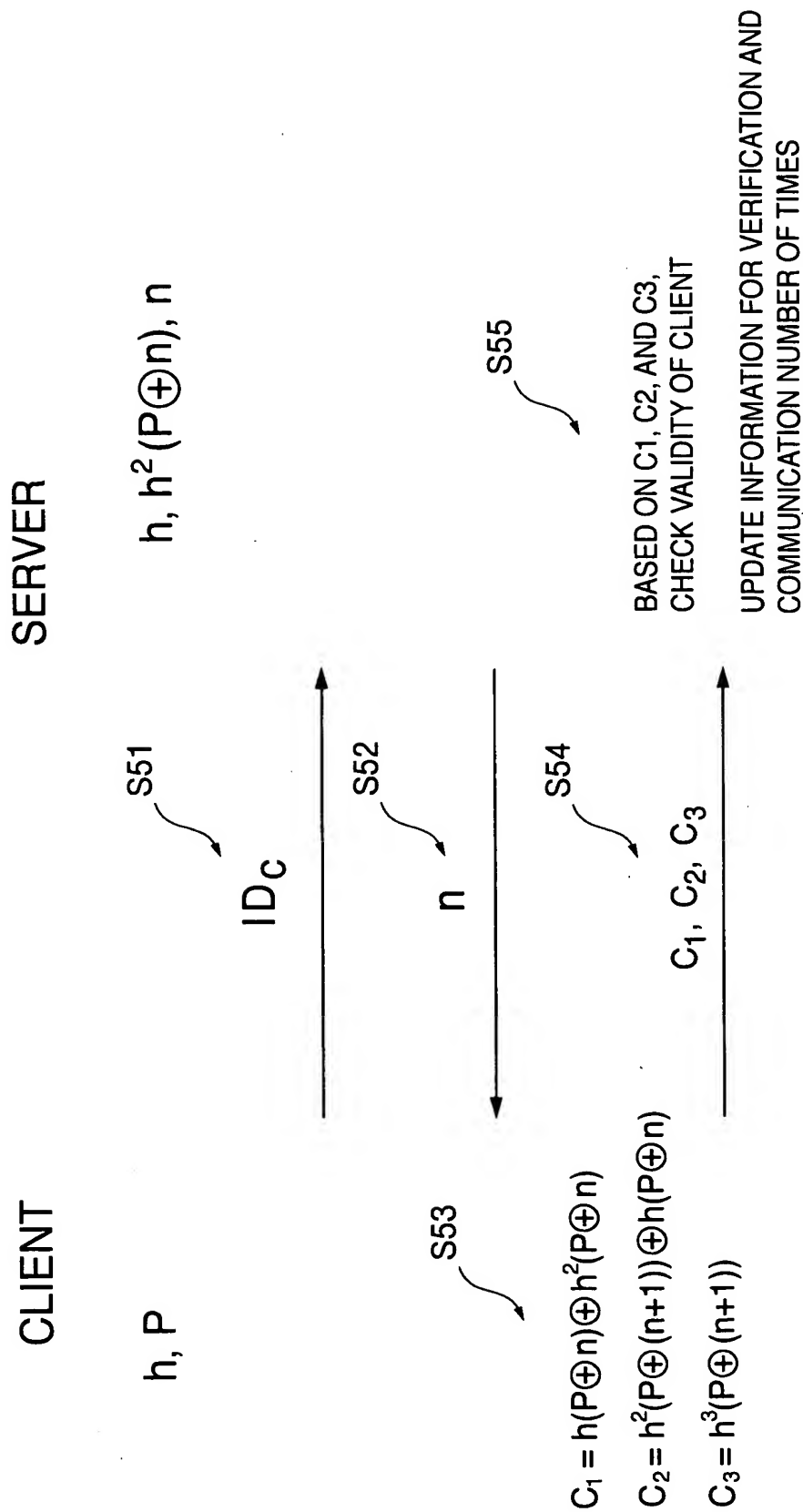


FIG.15

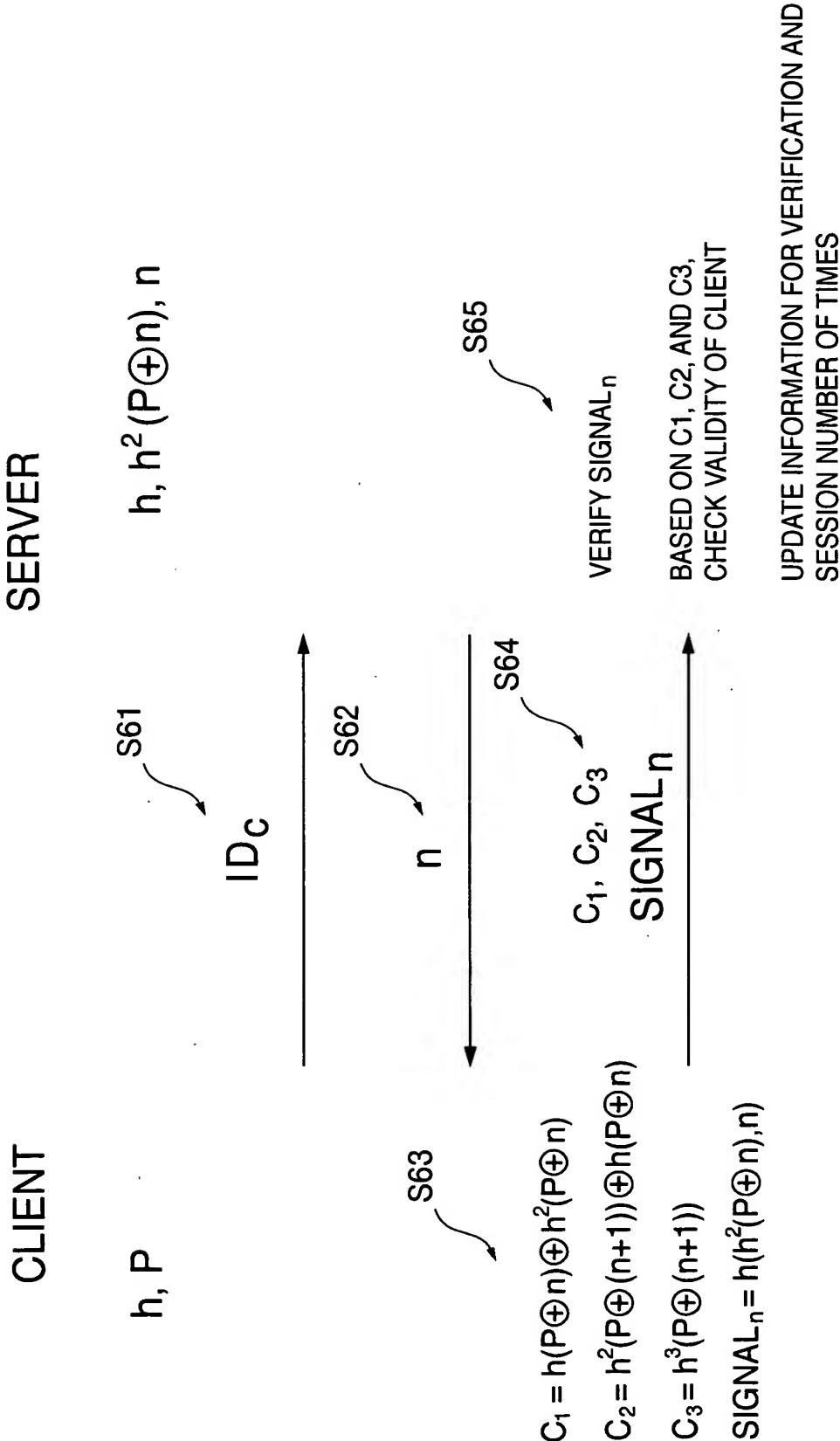


FIG.16

CLIENT

h, P, n

$$C_1 = h(P \oplus n) \oplus h^2(P \oplus n)$$

$$C_2 = h^2(P \oplus (n+1)) \oplus h(P \oplus n)$$

$$C_3 = h^3(P \oplus (n+1))$$

$$\text{SIGNAL}_n = h(h^2(P \oplus n), n)$$

S63

C_1, C_2, C_3

SIGNAL_n

S64

SERVER

$h, h^2(P \oplus n), n$

VERIFY SIGNAL_n

BASED ON C_1, C_2 , AND C_3 ,
CHECK VALIDITY OF CLIENT

UPDATE INFORMATION FOR VERIFICATION AND
SESSION NUMBER OF TIMES

S65

